AF$

MAIL STOP APPEAL BRIEF PATENTS
PATENT
8033-1024

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Shuji SHICHI	Conf. 1070
Application No. 09/883,371	Group 3692
Filed June 19, 2001	Examiner Harish Dass

DATA SALE IMMEDIATE SETTLING METHOD
AND PREPAID CARD

APPEAL BRIEF

MAY IT PLEASE YOUR HONORS:

(i) Real Party in Interest

The real party in interest in this appeal is the assignee, NEC Corporation of Tokyo, Japan.

(ii) Related Appeals and Interferences

None.

(iii) Status of Claims

Claims 1-15 were cancelled. Claims 16-35 are pending and rejected. Claims 16-35 were rejected by the Official Action mailed July 19, 2007 (the "Official Action"). The rejection of claims 16-35 is being appealed.

(iv) Status of Amendments

The Advisory Action of November 13, 2007 indicated that the After Final Amendment of October 19, 2007 would be entered for purposes of appeal.

(v) Summary of Claimed Subject Matter

Claims 16 and 30 are independent.

The claimed invention (as per claim 16) is a data sale immediate settling method (specification page 1, 14-8; Figures 1-5 generally).

The claimed invention provides a user with a prepaid card linked to a database (specification page 4, lines 12-22; Figure 1; specification page 5, line 22 - page 6, line 10).

The user executes a first action chain for immediately settling a data sale. The recited first action chain includes the sequential sub-steps of:

i) the user inputting a password number (specification page 2, lines 7-16; page 6, lines 5-10; page 7, line 22; action (6) of Figure 2),

ii) a first validation of the prepaid card by comparing the user-input password number to a system-set "first-time" password number stored on the database as the current password number (specification page 7, line 24 - page 8, line 4; action (7) of Figure 2),

iii) the user entering a "next-time" password number and storing the user-input next-time password number in the database as a new, user-set next-time password number (specification page 8, lines 5-23; actions (9-14) of Figure 2), and

iv) requesting a current monetary balance available on the prepaid card (specification page 9, lines 4-6; action (17) of Figure 2).

From the above, it can be seen that the invention requires the user to set a "next-time" password number for a next-time validation of the prepaid card. Further, this step is taken at a particular point in the method, i.e., i) after validation of the card by using a "first-time" password, and ii) prior to accessing the current monetary balance to actually use the prepaid card.

The claimed invention further requires repeating the user setting a next-time password each time the prepaid card is used. This simplifies use of the card for the user in that the user determines the next-time password and improves security/redundancy of the whole data sale settling network (specification page 11, lines 6-14).

The claim recites, in step C), executing another action chain comprising the sequential sub-steps of

i) the user inputting another password number (specification page 2, lines 7-16; page 6, lines 5-10; page 7, line 22; action (6) of Figure 2),

ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password number (specification page 7, line 24 - page 8, line 4; action (7) of Figure 2),

iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain (specification page 8, lines 5-23; actions (9-14) of Figure 2), and

iv) requesting another current monetary balance available on the prepaid card (specification page 9, lines 4-6; action (17) of Figure 2).

As discussed above, the claimed invention requires repeating of step C) where the user, with each use, sets a next-time password for use in the next-time validation of the prepaid card. This simplifies use of the card for the user and improves security/redundancy of the whole data sale settling network (specification page 11, lines 6-14).

The claimed invention (as per claim 30) is a data sale immediate settling method (specification page 1, 14-8; Figures 1-5 generally).

Claim 30 requires executing an immediate settling of a data sale action chain including validating a user's card by comparing a user-input password with a current password stored in a database, wherein, a first validation of the card uses a system-set first-time password stored on the database as the current stored password. See that the user inputs an initial password number (specification page 2, lines 7-16; page 6, lines 5-10; page 7, line 22; action (6) of Figure 2), which is used to validate of the prepaid card (specification page 7, line 24 - page 8, line 4; action (7) of Figure 2).

Claim 30 further recites that as part of each validation and prior to accessing a monetary balance of the user's card, the user sets a new user-set next-time password as the current next-time password stored in the database. As discussed above, the user sets a "next-time" password number which is stored in the database as a new, user-set next-time password number (specification page 8, lines 5-23; actions (9-14) of Figure 2), and subsequently there is a request for a current monetary balance available on the prepaid card (specification page 9, lines 4-6; action (17) of Figure 2). As in claim 16, the invention requires the user to set another "next-time" password number for each next-time validation of the prepaid card. Also as in claim 16, this step is taken at a particular point in the method, i.e., i) after validation of the card by using a "first-time" password, and ii) prior to accessing the current monetary balance and actually using the prepaid card.

As in claim 16, claim 30 requires that after the first validation of the card, subsequent validation of the card requires successful comparison of a current user input password to the stored current next-time password in the database (specification page 7, line 24 - page 8, line 4; action (7) of Figure 2).

(vi) Grounds of Rejection to be Reviewed on Appeal

A first ground of rejection presented for review on appeal is whether claims 16-21 and 30-33 were properly rejected as unpatentable under §103 as obvious over KWAN 2003/0200179 in view of PARRILLO 5,239,583.

A second ground of rejection presented for review on appeal is whether the remaining dependent claims were properly rejected as unpatentable under §103 as obvious, i.e., claims 22-26 and 29 as obvious over KWAN and PARRILLO in view of RUBIN 6,701,522; claims 27-28 and 34-35 as obvious over KWAN, PARRILLO, and RUBIN in view of NOVOA 6,636,973.

(vii) Arguments

Arguments Concerning the First Ground of Rejection

As to the first ground of rejection, claims 16-21 and 30-33 stand together.

The Examiner bears the initial burden of presenting a *prima facie* case of obviousness. *In re Oetiker,* 977 F.2d 1443, 1445 (Fed. Cir. 1992). If that burden is met, then the burden shifts to the Appellants to overcome the *prima facie* case with argument and/or evidence. *(See Id.)* In the present rejection, the Examiner has not satisfied this burden.

As discussed above, the present invention provides a user-supplied "next-time" password as part of each card validation and set by the user prior to accessing the card's monetary balance. A user-set password is a password set by the user and not a password set by the system.

See claim 16 step C)- sub-step iii) reciting the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain.

Also see step B) sub-step iii) which is similar.

The claims are not directed to merely replacing the password with each use of the prepaid card. The claims require specifically that the user provides and sets the password, the password being set at a particular point in the sequence of steps.

Since this concept is neither disclosed nor suggested by the prior art, one cannot say that this is an obvious concept.

KWAN teaches that the next-time password set by the merchant and the customer must accept the merchant-set code and later re-input the merchant-set code to validate the prepaid card.

This shortcoming in KWAN is not in dispute. Official Action (page 4, last line - page 5, line 8) acknowledges that KWAN does not disclose step B)- sub-step ii) or sub-step iii), or step C)- sub-step iii).

In performing the required obviousness analysis, the Examiner is required to make findings of fact and must provide an articulated reasoning supporting the rejection. The Examiner's articulated reasoning in the rejection must possess a rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

The Supreme Court citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) stated that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

The Examiner hasn't made sufficient findings of fact to support the rejection and rather relies on mere conclusory statements.

On pages 5-6 of the Official Action, there is a paragraph that lists "well known" actions. That these are well known now (i.e., in July 2007 when the Official Action was mailed) is not evidence that these actions were known to one skilled in the art at the time of the invention. It is clear error to rely on facts not supported by the record. A rejection including such clear error is improper.

In the last paragraph of Official Action page 6, the Examiner offers PARRILLO as teaching the user entering a next-time password as a new, user-set next-time password number.

This is a factual error as the PARRILLO password is not a user-set password as required by the claim. The PARRILLO Abstract discloses that the user enters a PIN code in accordance with a prescribed, but variable, sequence, the sequence being different for each transaction from the previous transaction. The user inputs the PIN by entering a sequence of alphanumeric symbols in accordance with a prescribed "start" sequence of symbols for recognition as a proper 4-digit PIN for a first transaction.

PARRILLO teaches that in "the broadest aspect of the invention, the user inputs the PIN by entering a sequence of alphanumeric symbols in accordance with a prescribed 'start' sequence of symbols for recognition as a proper 4-digit PIN for a first transaction". The system, upon recognizing the correct PIN, will give the user access to the account. See PARRILLO column 3, line 68 expressly teaches "At the same time, the system increments at least one of the digits of the stored PIN for that account so that, in effect, the user must enter a new PIN to access the same account on subsequent tries." See also beginning at line 12 of column 4.

From these passages, it is clear that the PARRILLO system is in control of setting and remembering the passwords.

What PARRILLO teaches is that each successful login by the user causes the system to increment to the next system-set password. It is this system-set password that must be entered in the PARRILLO system as part of the next transaction login.

Thus, although the PARRILLO user enters a different password for each transaction, it is a system-set password and not a user-set password. Thus, the step B), sub-step iii) and step C), sub-step iii) reciting of the user entering a new, user-set next-time password number is not disclosed or suggested.

Further, claim 16 requires that the user enter this next-time password prior to sub-step iv) of requesting a current monetary balance available on the prepaid card number. In PARRILLO, the teaching is that, upon a successful login "at the same time, the system increments at least one of the digits of the stored PIN" (line 68 of column 3 and line 1 of column 4). This action does not involve the user inputting the next-time password. PARRILLO allows the transaction (including step iv) and only thereafter when the user wishes to make another transaction is the next-time password input by the user (corresponding to step C), sub-step i).

Additionally, although PARRILLO teaches that the system increments the PIN, there is no disclosure that the system stores the new PIN (the sequence of PINs may be pre-established and incrementing moves from on PIN to a new previously stored PIN).

Further, step B), sub-step iii) and step C), sub-step iii) explicitly require "storing the user-input next-time password number in the database as a new, user-set next-time password number," (again prior to sub-step iv). Thus, even if a new password were stored in PARRILLO, the new password is not a user-input password as required by the claim.

Nor is there any teaching of the user-input and storing of the user-input next-time password number sub-step being performed prior to requesting a current monetary balance available on the prepaid card during a current transaction.

In this regard, PARRILLO, KWAN, and NOVOA 6,636,973 are the same in that the user does not set the password.

See in NOVOA column 3, lines 6-25 it is disclosed, beginning at line 15, (emphasis added) "At some point during or after the log on process, a biometrics account manager which has access to the users database changes the current password associated with the use to a new password. Because the user is not required to remember and type the password, the passwords may be longer and more complex, thereby further enhancing security." If the user is not required to remember the password, it is clear that the user need not enter the new password at a later time. This passage explicitly states that the user does not type the password.

See column 3, lines 26-30 stating that the password is generated randomly. See also column 9, lines 2-9. The new password is used to log on the user; however, the user does not enter the new password. Additionally, the user does not select or enter the next-time password into the system during the current password validation.

Thus, each of these references teaches completely opposite to the recited invention where, the present invention provides that the user inputs, at each and every use, a new next-time password after entering and verifying the current password and prior to accessing the monetary balance on the prepaid card.

In conclusion, the Examiner's rejection fails to present an articulated reasoning, based on facts of record, that provide a rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d at 988. Without such articulated reasoning, based on proper facts, there is no support for the legal conclusion of obviousness.

Thus, the Examiner has not established obviousness because the applied references neither teach nor would have suggested to the skilled artisan the proposed modification of KWAN necessary to arrive at the recited invention.

The rejection is therefore improper.

Arguments Concerning the Second Ground of Rejection

As to the second ground of rejection, the claims stand together.

Each of these further claims is improperly rejected because they depend from an allowable claim.

Conclusion

Reversal of the obviousness rejections is earnestly requested.

Respectfully submitted,

YOUNG & THOMPSON

By

Roland E. Long, Jr.
Attorney for Appellant
Registration No. 41,949
209 Madison Avenue
Suite 500
Alexandria, VA 22314
Telephone: 703/521-2297

April 7, 2008

(viii) Claims Appendix

16. A data sale immediate settling method comprising the sequential steps of:

A) providing a user with a prepaid card linked to a database;

B) executing a first action chain for immediately settling a data sale comprising the sequential sub-steps of

i) the user inputting a password number,

ii) a first validation of the prepaid card by comparing the user-input password number to a system-set first-time password number stored on the database as the current password number,

iii) the user entering a next-time password number and storing the user-input next-time password number in the database as a new, user-set next-time password number, and

iv) requesting a current monetary balance available on the prepaid card; and

C) executing another action chain comprising the sequential sub-steps of

i) the user inputting another password number,

ii) validation of the prepaid card by a successful comparison of the user-input another password number to the stored new, user-set next-time password number,

iii) the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain, and

iv) requesting another current monetary balance available on the prepaid card,

wherein step C) is repeated.

17. The method of claim 16, wherein the prepaid card is a virtual card.

18. The method of claim 16, wherein,

the prepaid card comprises a physical card carrying duplicate information carried in the database,

the prepaid card comprises a serial number, the first-time password number, and an expiration date printed on an exterior surface of the physical card, and

the database comprises the serial number, the first-time password number, and the expiration date of the prepaid card.

19. The method of claim 18, wherein,

the first-time password number is concealed below of scratch-off covering.

20. The method of claim 16, wherein,

the database includes a database record corresponding to the prepaid card and comprising a serial number field storing a system-assigned serial number, a first-time password number field storing the system-assigned first-time password number used for a first time validation of the prepaid card, and a user-set password number field for storing the user-set next-time password number reset by the user subsequent to each validation of the prepaid card, a monetary balance field storing a monetary balance available to the user, and

comprising the further step of:

subsequent to the validation of the prepaid card, a action of subtracting a price being necessary for distribution from monetary balance field to update the monetary balance field by reducing a value of the monetary balance field by the price being subtracted.

21. The method of claim 20, wherein, the database record further comprises:

an issue date field, an expiration date field, a card monetary face value field, a transaction product/service number field, and a transaction date field, each having a one-to-one correspondence with the prepaid card.

22. The method of claim 20, comprising the further steps of:

a portal site, located between a user and the database, receiving from the user an input of the card serial number and the user input another password number;

the portal accessing the database and validating the prepaid card by comparing the received user-input another password number with the next-time password number stored on the database.

23. The method of claim 22, wherein the portal site is connected to the user and to the database via the Internet.

24. The method of claim 22, wherein the portal site is connected to the user via a telephone line.

25. The method of claim 24, wherein the user orally inputs the another password number to the portal.

26. The method of claim 23, wherein,

the portal site further receives user input of the serial number and confirms the expiration date of the prepaid card to the database prior to validating the prepaid card.

27. The method of claim 26, wherein,

after validation of the prepaid card, the portal site i) requests the user to input the new user-set next-time password number, ii) receives the new user-set password number from the user, iii) sends the received new user-set next-time password number to the database to be stored, in the user-set next-time password number field, as the next-time password number required for a next validation of the prepaid card.

28. The method of claim 26, wherein,

a next successful validation of the prepaid card requires the portal site i) to receive from the user the another password number input, and ii) to successfully compare the received another password number input with the next-time password number stored in the user-set password number field of the record of the prepaid card within the database.

29. The method of claim 24, wherein the user orally inputs the password number to the portal site and the portal site orally responds to the user, via a telephone call.

30. A data sale immediate settling method comprising the steps of:

executing an immediate settling of a data sale action chain including validating a user's card by comparing a user-input password with a current password stored in a database, wherein,

a first validation of the card uses a system-set first-time password stored on the database as the current stored password,

as part of each validation and prior to accessing a monetary balance of the user's card, the user sets a new user-set next-time password as the current next-time password stored in the database, and

after the first validation of the card, subsequent validation of the card requires successful comparison of a current user input password to the stored current next-time password in the database.

31. The method of claim 30, wherein,

the card comprises a physical card carrying duplicate information carried in the database, and

the card each comprises a serial number, the first-time password number, and an expiration date printed on an exterior surface of the physical card.

32. The method of claim 30, wherein,

the database includes a database record corresponding to the card and comprising a serial number field storing a system-assigned serial number, a first-time password field storing the system-assigned first-time password used for a first time validation of the card, and a user-set password field for storing the user-set next-time password reset as the current next-time password number by the user subsequent to each validation of the card, a monetary balance field storing a monetary balance available to the user, and

comprising the further step of:

subsequent to the validation of the card, a action of subtracting a transaction price for distribution to a vendor from the monetary balance field to update the monetary balance field by reducing a value of the monetary balance field by the price being subtracted.

33. The method of claim 32, wherein, the database record further comprises:

an issue date field, an expiration date field, a card monetary face value field, a transaction product/service number field, and a transaction date field, each having a one-to-one correspondence with the card.

34. The method of claim 32, comprising the further steps of:

a portal site, located between a user and the database, receiving from the user an input of the card serial number and the user input password;

the portal accessing the database and validating the card by comparing the received user-input password with the current next-time password stored on the database.

35. The method of claim 34, wherein,

after validation of the card, the portal site i) requests the user to input the new user-set next-time password, ii) receives the new user-set next-time password from the user, iii) sends the received new user-set next-time password to the database to be stored, in the user-set password field, as the current next-time password required for a next validation of the card.

(ix) Evidence Appendix

None.

(x) Related Proceedings Appendix

None.